INTERNATIONAL JOURNAL OF LAW: **"LAW AND WORLD"**
December 2020 (№15). Volume 6; Issue 2; Page No.145-157
https://doi.org/10.36475/6.2.12
www.lawandworld.ge
ISSN: 2346-7916 (Print); ISSN: 2587-5043 (Online)



Socio-economic analysis of cybercrime

Irakli Nadareishvili
Doctor of Law, Assistant professor of Caucasus International University,
Head of The Department to Investigate, Offenses Committed in the Course of Legal Proceedings, The Office of The General Prosecutor of Georgia

Jemal Lomsadze
Master of Law. Senior Prosecutor of The Department, to Investigate, Offenses Committed in the Course of Legal Proceedings, The Office of The General Prosecutor of Georgia

ABSTRACT

In the presented article, the author analyzes socio-economic damage caused and expected as a result of cybercrime, a global and transnational threat. In parallel, with the development of technology and the growing dependence of the population on internet resources in the digital era, there are discussed dangers of blooming opportunities for cybercriminals and harm imposed by their actions. Taking into account the scale of the proceeds of crime, the author of the article presumes that cybercrime has formed into organized criminal business and has become a threat not only to the security of states and proper functioning of their institutions but also to the property and assets of citizens and enterprises, banks and fund institutions. According to the author, even the rules implemented by countries with a strong economy and developed technologies, and the refinement/ development of methods to combat this crime, will not bring results and will not be effective, since cybercrime is global and transnational by its nature. To accomplish the goals effectively, response to this challenge should be comprehensive, based on unified, well-established international policy. This only can be achieved through close interstate cooperation and instant (bypassing bureaucratic formalism) mutual legal assistance.

KEYWORDS: Cybercrime, Hacker, Virus

BIBLIOGRAPHY:

1. Tsatsanashvili M., Sikharulidze T., Problems of cyberterrorism in Law, e. Journal "Cyber Security", 2007. http://informsoc.org/ka/journal/cybersecurity/69-2009-08-19-15-33-04 (In Georgian)
2. Kokhreidze N. "Cybercrime". http://ilawge.blogspot.com/2012/05/blog-post_191.html (In Georgian)
3. Kokhreidze N., "Cyber Capabilities of Russia" (research) http://ilawge.blogspot.com/2013/01/blog-post.html (In Georgian)
4. Lanchava G. "Computer Crime", Journal "Justice", N2, 2008 (In Georgian)
5. Yar M., Steinmetz K.F., Cybercrime and Society, Third Edition, SAGE Publishing Ltd, London, 2019 (In English)
6. United Nations Office on Drugs and Crime, The Globalization of Crime, A Transnational Organized Crime Threat Assessment, United Nations publication, Vienna, 2010, ISBN: 978-92-1-130295-0 (In English)

https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf
7. The LexisNexis® Risk Solutions Cybercrime Report https://risk.lexisnexis.com/global/-/media/files/financial%20services/research/lnrs-cybercrime-report-research-january-june-2019.pdf
8. Cybersecurity Ventures, 2017. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (In English)
9. The independent IT-security institute, AV-TEST GmbH, Magdenburg, Germany https://www.av-test.org/en/statistics/malware/ (In English)
10. Jansen J., Leukfeldt R., Coping with cybercrime victimization: An exploratory study into impact and change, Journal of Qualitative Criminal Justice and Criminology, volume 6, Number 2, Special Issue, Dallas, 2018 https://www.jqcjc.org/documents/v6i2.pdf#page=78 (In English)
11. Sumanjit D., Tapaswini N., Impact of Cyber Crime: Issues and Challenges, International Journal of Engineering Sciences & Emerging Technologies, Volume 6, Issue 2 (In English) http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
12. Understanding the costs of cyber crime, A report of key findings from the Costs of Cyber Crime Working Group, Research Report 96, Home Office Science Advisory Council, January 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf (In English)
13. Federal Bureau of Investigation Internet Crime Complaint Center, 2019 crime complaint report. https://pdf.ic3.gov/2019_IC3Report.pdf (In English)
14. 2019 International Cybersecurity Congress report https://icc.moscow/upload/doc/ICC_reports_EN.pdf (In English)

კიბერდანაშაულის სოციალურ-ეკონომიკური ანალიზი

ირაკლი ნადარეიშვილი

სამართლის დოქტორი, კავკასიის საერთაშორისო უნივერსიტეტის ასისტენტ პროფესორი, საქართველოს გენერალური პროკურატურის სამართალწარმოების პროცესში ჩადენილი დანაშაულის გამოძიების დეპარტამენტის უფროსი

ჯემალ ლომსაძე

სამართლის მაგისტრი, საქართველოს გენერალური პროკურატურის სამართალწარმოების პროცესში ჩადენილი დანაშაულის გამოძიების დეპარტამენტის უფროსი პროკურორი

საკვანძო სიტყვები: კიბერდანაშაული, ჰაკერი, ვირუსი

შესავალი

ორ ათწლეულზე ნაკლებ დროში, ინტერნეტი საინტერესო სიახლიდან გადაიზარდა მილიონობით ადამიანის ცხოვრების მნიშვნელოვან ასპექტად. გლობალიზაციის სხვა გამოვლინებებთან ერთად, ინტერნეტის სწრაფმა განვითარებამ მკვეთრად გადააჭარბა მისი კონტროლის შესაძლებლობებს, მეთვალყურეობის ნაკლებობამ კი გაადვილა ინტერნეტის შესაძლებლობების ბოროტად, დანაშაულის მიზნებისათვის გამოყენება. აღნიშნული სირთულეს კიდევ უფრო ამწვავებს ის ფაქტი, რომ ინტერნეტი შეიქმნა სამხედრო სისტემის ბაზაზე, რომელიც მიმართული იყო წინაღობების და გარე კონტროლი მექანიზმების დაძლევისკენ. დღეის მდგომარეობით ისინიც კი ვინც ხმამაღლა იცავდნენ ინტერნეტის შემოქმედებით ანარქიას მიხვდნენ, რომ ინტერნეტის პოტენციალის სრულფასოვნად ათვისება და მისი საზოგადოებისათვის სასარგებლო სამსახურში ჩაყენება შეუძლებელია ძირითადი წესების დადგენის, ანტისაზოგადოებრივი ქცევების დაგმობისა და მკაცრი საკანონმდებლო რეგულაციების დაწესების გარეშე. ინტერნეტის საშუალებით განხორციელებულ დანაშაულთა შედეგად მიყენებული, ყოველწლიურად მზა-

რდი ზიანი კოლოსალურ მასშტაბებს აღწევს და დამანგრეველი ეფექტი აქვს, როგორც სახელმწიფო უსაფრთხოების კუთხით, ისე მსოფლიოს სოციალურ-ეკონომიკურ სტაბილურობის მიმართებით.

კიბერდანაშაულის სოციალურ-ეკონომიკური ანალიზი

კიბერდანაშაული არ განეკუთვნება სისხლის სამართლის კლასიკურ დელიქტს, ისეთს, როგორიც არის მკვლელობა, ყაჩაღობა, ქურდობა და ა.შ. XXI საუკუნეში განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად დაგვანახა კიბერუსაფრთხოების პოლიტიკის შემუშავების აუცილებლობა, რათა უზრუნველყოფილ იქნას სტრატეგიულად მნიშვნელოვანი ობიექტების, კომპიუტერული სისტემების გამართული და უსაფრთხო ფუნქციონირება. კომპიუტერული ტექნოლოგიების განვითარებამ მნიშვნელოვნად განაპირობა მსოფლიოს კიბერსივრცეში გამოწვევების, რისკების, საფრთხეების, მათი წყაროების წარმოქმნა და აღნიშნულიდან გამონაკლისს არც საქართველო წარმოადგენს.

ინტერნეტსივრცის შექმნასთან ერთად, გაჩნდა ისეთი ცნებები, როგორებიცაა კიბერსივრცე, კიბერდანაშაული, კიბერტერორიზმი, კიბერომი, კიბერუსაფრთხოება და სხვა. ყველა ჩამოთვლილ მოვლენას ინტერნეტის – გლობალური კომპიუტერული ქსელის შექმნა უდევს საფუძვლად. ინტერნეტი თავდაპირველად მოწინავე კვლევითი სააგენტოების (ARPA) და ამერიკის შეერთებული შტატების (აშშ) თავდაცვის დეპარტამენტის (DOD) მიერ 1969 წელს შეიქმნა არპანეტის (ARPANET) სახით და მიზნად ისახავდა, ელექტრონული კვანძების გამოყენებით, ოთხი ამერიკული უნივერსიტეტისა და მათ მეცნიერთა ერთმანეთთან დაკავშირებას.[1] თუმცა, დღეისათვის, ინტერნეტი მთელ მსოფლიოს მოიცავს და მან შეაღწია თითქმის ყველა ოჯახში. პირველად, 2001 წლის 11 სექტემბრის მოვლენებმა აიძულა მსოფლიო, ყურადღება გაემახვილებინა ინტერნეტის გამოყენების არამხოლოდ დადებით შედეგებზე, არამედ ისეთ სერიოზულ საფრთხეებსა და რისკებზე, რომლებიც შესაძლოა კიბერსივრციდან მომდინარეობდეს. სწორედ ასეთი რისკების გაანალიზების შემდეგ, კაცობრიობა დადგა კიბერსივრცის სამართლებრივი რეგულირებისა და კიბერდანაშაულის აღსაკვეთად მნიშვნელოვანი სტრატეგიების დანერგვის აუცილებლობის წინაშე.

ყურადღებას გავამახვილებთ კიბერდანაშაულის შემდეგ სახეებზე:

1. ბავშვთა პორნოგრაფია – შემთხვევა, როდესაც კიბერსივრცის გამოყენებით, ჩათისა (Chat) თუ სხვა პროცესის განმავლობაში ხდება არასრულწლოვნის ჩაბმა და დაყოლიება სექსუალური ხასიათის უკანონო ქმედებებში. ასევე, ისეთი მასალის შექმნა და გავრცელება, რომელიც უარყოფით ზეგავლენას ახდენს არასრულწლოვნებზე.
2. კიბერგათეთრება – არანაკლებ გავრცელებული დანაშაული, როდესაც ინტერნეტის გამოყენებით ხდება უკანონოდ მოპოვებული ფულის გათეთრება, გადარიცხვა სხვადასხვა საიტებზე, შესაბამისი პიროვნებების ვინაობის მითითების გარეშე.
3. კიბერქურდობა და კიბერთაღლითობა – ქურდობა/თაღლითობა, სხვისი ქონების ფარული ან/და მოტყუებით დაუფლება კომპიუტერული სისტემისა და ინტერნეტის გამოყენებით.
4. კიბერვანდალიზმი – საინფორმაციო ბაზებში შეღწევა და მათი განადგურება, რა დროსაც დამნაშავის მიზანს არ წარმოადგენს მონაცემის მოპარვა, ან რაიმე მიზნით გაცნობა.
5. კიბერტერორიზმი, კიბერდანაშაულის ერთ-ერთი ყველაზე საშიში ფორმა. კიბერტერორიზმი – ეს არის კომპიუტერზე, ქსელზე და მათში არსებულ ინფორმაციაზე შეტევის ან შეტევის განხორციელების მუქარა, სახელმწიფო, ან მისი ხალხის პოლიტიკურად, სოციალურად, რელიგიურად ან იდეოლოგიურად დაშინების მიზნით.

ტერმინი „კიბერტერორიზმი“ პირველად 1980 წელს კალიფორნიის უსაფრთხოებისა და დაზვერვის ინსტიტუტის მეცნიერ-თანამშრომელმა, ბარი კოლინმა გამოიყენა. მისი პირველი განმარტება კი FBI-ს ოფიციალურმა აგენტმა, მარკ პოლიტმა გააკეთა, რომელმაც აღნიშნა, რომ კიბერტერორიზმი ეს არის სუბნაციონალური, ან ფარული აგენტების მიერ წინასწარ განზრახული, პოლიტიკურად მოტივირებული ძალადობა მშვიდობიანი (არამებრძოლი) სამიზნის წინააღმდეგ, რაც გამოხატულია ინფორმაციაზე, კომპიუტერულ სისტემებზე, პროგრამებსა და მონაცემთა ბაზებზე შეტევასა და

1 ცაცანაშვილი მ., სიხარულიძე ტ., კიბერტერორიზმის პრობლემები სამათალში, ელ. ჟურნალი «კიბერუსაფრთხოება", 2007, იხ. http://informsoc.org/ka/journal/cybersecurity/69-2009-08-19-15-33-04

მათ განადგურებაში. აშშ-ს კიბერტერორიზმის ერთ-ერთმა ექსპერტმა, ჯორჯთაუნის პროფესორმა დოროთი დენინგმა, ინტერნეტში საქმიანობის კლასიფიკაციის სამი ასპექტი გამოყო. ეს არის: 1. „აქტივიზმი" – კიბერსივრცის "ლეგიტიმური" (მისი ტერმინებით ნორმალური) გამოყენება საკუთარი იდეების პროპაგანდისა თუ სხვა ღონისძიებების განხორციელების მიზნით, რომელიც მოიცავს ინფორმაციის მოძიებას, ინტერნეტგვერდების განთავსებას, ელ-ფოსტის გამოყენებას, ელექტრონული პუბლიკაციების გავრცელებას. აგრეთვე, ინტერნეტის გამოყენებას სხვადასხვა საკითხის განსახილველად, კოალიციების შესაქმენალად ან ქმედებათა კოორდინაციას. 2. „ჰაკტივიზმი" – მოიცავს ოპერაციებს, როდესაც გამოიყენება „ჰაკერების" ტექნიკა სამიზნის ვებგვერდის წინააღმდეგ და მის მთავარ მიზანს წარმოადგენს ნორმალური ფუნქციონირებისათვის ხელის შეშლა და არა დამანგრეველი ზიანის მიყენება. ამის მაგალითებია: ვირტუალური ბლოკადა, კომპიუტერული "ტროიანები" და ვირუსები, ავტომატური ელ-ფოსტის „დაბომბვა", კომპიუტერების „გატეხვა" და ა.შ. და ბოლოს 3. „კიბერტერორი", რაც წარმოადგენს ტერორიზმისა და კიბერსივრცის შერწყმას. ის მოიცავს პოლიტიკურად მოტივირებულ ჰაკერულ ოპერაციებს, რომელთა მიზანია დამანგრეველი შედეგის მიღწევა, როგორიც არის ლეტალური ან მძიმე ეკონომიკური შედეგები. [2]

კომპიუტერული სისტემების განვითარებამ და ე.წ. „ჰაკერული" თავდასხმების დახვეწამ განაპირობა სხვადასხვა საწარმოებისა და ორგანიზაციების მისწრაფება, საკუთარ კომპანიაში დანერგონ მაღალი ხარისხის კომპიუტერული მონაცემების დამცავი ტექნოლოგიები. თავის მხრივ, კიბერდამნაშავეები ცდილობენ იპოვონ კიბერშეტევებისგან ნაკლებად დაცული სივრცე. უსაფრთხოების ექსპერტების მტკიცებით, მასობრივი კიბერშეტევების მორიგი ტალღა აუცილებლად განხორციელდება სხვადასხვა სახის სოციალური ქსელების მეშვეობით, რომლებიც ძალიან დიდი პოპულარობით სარგებლობენ თანამედროვე მსოფლიოში.

სოციალური ქსელები, როგორებიც არის – Facebook, LinkedIn და Twitter, საზოგადოებაში ძალიან ფართოდ არის გავრცელებული. სოციალური ქსელების გამოყენებით ადამიანები ურთიერთობენ საკუთარ ოჯახთან, მეგობრებთან, უზიარებენ ერთმანეთს სხვადასხვა სახის გამოცდილებას. სოციალური ქსელები, აქტუალობიდან გამომდინარე, ასევე, იქცა პოლიტიკურ „იარაღად".

სახელმწიფოები და წამყვანი ბიზნეს ორგანიზაციები უკვე აღიარებენ სოციალური ქსელების უპირატესობას სხვადასხვა საკითხებში, თუმცა უნდა აღინიშნოს, რომ სოციალურ ქსელების გამოყენება კომპანიებს უქმნის უზარმაზარ რისკს და გზას უხსნის კიბერდამნაშავეს გამოიყენოს სხვადასხვა ტექნოლოგიები კიბერ-შეტევის განსახორციელებლად.

ერთ-ერთ ყველაზე ნათელ მაგალითს იმისა, თუ რა სახის ზიანი შეიძლება მოიტანოს სოციალური ქსელების გამოყენებით განხორციელებულმა კიბერდანაშაულმა წარმოადგენს „შარმიანი კნუტის" სახელწოდებით ცნობილი კიბერშეტევა. აღნიშნული კიბერშეტევის ორგანიზება მოხდა ირანის სახელმწიფოში და მის ძირითად სამიზნეს წარმოადგენდნენ აშშ-ს სამხედრო და დიპლომატიური პირები, კონგრესის წევრები, ჟურნალისტები და აშშ-ს მოკავშირე სახელმწიფოების თანამდებობის პირები. „შარმიანი კნუტის" კიბერშეტევის ფარგლებში კიბერდამნაშავეებმა სხვადასხვა სოციალურ ქსელებში (Facebook, LinkedIn, Twitter და Google +) ყალბი მონაცემებით დაარეგისტრირეს ათეულობით მომხმარებელი, რომლებიც ცდილობდნენ, სხვადასხვა თანამდებობის პირებთან დაემყარებინათ ახლო-მეგობრული ურთიერთობები, რასაც შემდგომ გამოიყენებდნენ აღნიშნული პირების კომპიუტერულ სისტემაში სხვადასხვა სახის ვირუსული პროგრამის გასავრცელებლად და ამ პირების კომპიუტერული სისტემიდან მათთვის სასურველი ინფორმაციის მისაღებად.

მიუხედავად იმისა, რომ სოციალური ქსელები საზოგადოებაში აქტუალური გახდა ბოლო რამდენიმე წლის განმავლობაში, ისტორიულად ცნობილია, რომ პირველი ფაქტი, როდესაც კიბერდამნაშავეებმა სოციალური ქსელი გამოიყენეს საზოგადოებაში პანიკის დათესვის მიზნით, განხორციელდა რუსეთის ფედერაციაში დაახლოებით 15 წლის წინ. ე.წ. „ჰაკერებმა" (Hacker – პიროვნება, რომელიც ეძებს და დანაშაულებრივი მიზნებისთვის იყენებს სხვის კომპიუტერულ სისტემაში არსებულ ხარვეზებს) კიბერშეტევა განახორციელეს ატომური ელექტროსადგურის ოფიციალურ ვებ-გვერდზე და საზოგადოებაში, სოციალური ქსელების გამოყენებით, გაავრცელეს ინფორმაცია, თითქოს ატომურ ელექტროსადგურზე მოხდა გაჟონვა, რამაც გარკვეული პერიოდით მოსახლეობაში პანიკა და ქაოსი გამოწვია.

---

2 ცაცანაშვილი მ., სიხარულიძე ტ., კიბერტერორიზმის პრობლემები სამათალში, ელ. ჟურნალი «კიბერ უსაფრთხოება", 2007, იხ. http://informsoc.org/ka/journal/cybersecurity/69-2009-08-19-15-33-04

სოციალური ქსელების მეშვეობით ფართოდ გავრცელებულ კიბერდანაშაულებს შორის გამოყოფენ:

ა) ე.წ. „ცრუ შეთავაზებებს", როდესაც სოციალური ქსელის მომხმარებელი იღებს შეტყობინებას და მის სანახავად აუცილებელია სხვადასხვა სახის პირადი ინფორმაციის შევსება, რომლის შევსების შემთხვევაში აღნიშნული ინფორმაცია ავტომატურად ხვდება კიბერდამნაშავესთან;

ბ) ე.წ. „მოწონების ღილაკი", რაც არის კიბერდამნაშავის მიერ შექმნილი ერთგვარი „ხაფანგი", რაც გათვლილია იმაზე, რომ თუ სოციალური ქსელის მომხმარებელი დააჭერს ე.წ. „მოწონების ღილაკს", მის კომპიუტერში ავტომატურად იტვირთება მავნე პროგრამა, რომელიც, თავის მხრივ, კიბერდამნაშავეს საშუალებას აძლევს შეაღწიოს მომხმარებლის კომპიუტერულ სისტემაში. ანალოგიური სახის კიბერშეტევის საშიშროებასთან გვაქვს საქმე, როდესაც მომხმარებელი ცდილობს სხვადასხვა ვებ-გვერდიდან გადმოიწეროს რომელიმე პროგრამის აპლიკაცია, რაც სინამდვილეში წარმოადგენს საფრთხის მატარებელ პროგრამას. მისი გადმოტვირთვის შემთხვევაში კიბერდამნაშავეს შეუძლია შეაღწიოს კონკრეტული პირის კომპიუტერულ სისტემაში და გადმოტვირთოს მისთვის სასურველი ინფორმაცია.

ზოგადად ტერმინი „კიბერდანაშაული" გამოიყენება დანაშაულთა ფართო სპექტრის მიმართ, მათ შორის არის კომპიუტერული მონაცემებისა და სისტემების წინააღმდეგ მიმართული ქმედებები (როგორიცაა ჰაკერობა), ინტერნეტ რესურსებთან დაკავშირებული თაღლითობა და სიყალბე (ე.წ. „ფიშინგი"), ბავშვთა პორნოგრაფიის გავრცელება და საავტორო უფლებების დარღვევა (პირატული ნაწარმის გავრცელება) და სხვა. კიბერდანაშაული, ცალმხრივი მავნებლური კიბერ-ვანდალიზმიდან, ძალიან მალე გადაიზარდა საკმაოდ შემოსავლიან დანაშაულებრივ საქმიანობაში. რა თქმა უნდა კრიმინალებიც, ისევე როგორც რიგითი ადამიანები, იყენებენ ინტერნეტს კომუნიკაციისთვის და ინფორმაციის შეგროვებისთვის, რამაც თავის მხრივ ხელი შეუწყო ტრადიციული ორგანიზებული დანაშაულის განვითარებას. ინტერნეტის მნიშვნელობის ზრდამ და მასზე ჩვენმა ყოველდღიურმა, მასობრივმა დამოკიდებულებამ წარმოშვა ახალი დანაშაულებრივი შესაძლებლობები.

გაერთიანებული ერების ორგანიზაციის ნარკოტიკისა და დანაშაულის სამმართველოს 2010 წლის ანგარიშში, რომელიც შეეხებოდა დანაშაულის გლობალიზაციისა და ტრანსნაციონალური ორგანიზებული დანაშაულის საფრთხის შეფასების საკითხს, აღნიშნულია, რომ ყველაზე პრობლემურად მიჩნეული უნდა იქნას: თაღლითობა პირადი მონაცემების მიტაცების გზით, ნარკორეალიზაცია ინტერნეტრესურსების გამოყენებით და ბავშვთა პორნოგრაფიით ვაჭრობა. ანგარიშის მიხედვით მთავარი საკვანძო საკითხი მდგომარეობს იმაში, რომ ეს დანაშაულებრივი საქმიანობა უნდა მივიჩნიოთ ორგანიზებულ დანაშაულად. მრავალ უპირატესობას შორის, რასაც კიბერსივრცე სთავაზობს დამნაშავეებს, არის ანონიმურობა და შესაძლებლობა მსოფლიოს სხვადასხვა კუთხეში მყოფი ადამიანები დაუკავშირდნენ ერთმანეთს ტრანსნაციონალურ დონეზე (მაგალითად ფორუმებისა და ე.წ „ჩათების" მეშვეობით). ამასთან გამოთქმულია შეშფოთება, რომ საფუძვლიანი ვარაუდით მოსალოდნელია ორგანიზებული კიბერდანაშაულის ახლო მომავალში კიდევ უფრო მომძლავრება.[3]

პირველ რიგში უნდა აღინიშნოს, რომ ბოლო ათწლეულში კიბერდანაშაულის ჩასადენად საჭირო ტექნოლოგიები გაცილებით უფრო ხელმისაწვდომი გახდა. ინტერნეტის მეშვეობით შესაძლებელია პროგრამული უზრუნველყოფის შეძენა, რომელიც საშუალებას აძლევს მომხმარებელს მოიძიოს ღია პორტები და შეაღწიოს დაცულ სისტემებში. აღნიშნული საშუალებები გაცილებით უფრო აფართოებს პოტენციური კანონდამრღვევების არეალს და დანაშაულის ჩადენა შესაძლებელი გახდა იმათთვისაც, ვისაც არ გააჩნია განსაკურებული კომპიუტერული უნარები. მაგალითისთვის, არც თუ ისე დიდი ხნის წინ აღმოჩენილი, ისტორიაში ყველაზე მძლავრი ბოტნეტი (შეპყრობილი კომპიუტერების ქსელი) „მარიპოსა", შექმნილი იყო არც თუ ისე კვალიფიციური ჰაკერების მიერ. მსგავსი სახის პროგრამული უზრუნველყოფის ხელმისაწვდომობის შეზღუდვა რთულია, ხშირ შემთხვევაში მისი გავრცელება ხდება ხელიდან-ხელში, ან ე.წ. „მირორინგის", ანუ დუბლირების მეშვეობით. კვალიფიციურ კიბერ-ქურდებს, როგორც წესი, კონკრეტული ორგანიზაციისთვის მუშაობას ურჩევნიათ დამოუკიდებლად მუშაობა. თავის მხრივ კრიმინალური დაჯგუფებები სპეციალური პროგრამების გამოყენებით ასაქმე-

3 United Nations Office on Drugs and Crime, The Globalization of Crime, A Transnational Organized Crime Threat Assessment, United Nations publication, Vienna, 2010, ISBN: 978-92-1-130295-0, pp 203-204 https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

ბენ ნაკლებად სპეციალიზებულ პირთა ფართო წრეს, რთავენ მათ დანაშაულებრივ საქმიანობაში და იყენებენ თავიანთი მიზნების მისაღწევად. მეორე ფაქტორი, რაც ხელს უწყობს კიბერდანაშაულის განვითარებას, არის ინტერნეტის მომხმარებელთა რიცხობრივი ზრდა. 2005 წელს, განვითარებად ქვეყნებში ინტერნეტის მომხმარებელთა რიცხვმა, გადააჭარბა ინდუსტრიულ ქვეყნებში მომხმარებელთა რაოდენობას. ახალ მომხმარებელთა შორის გვხვდება ბევრი პოტენციური დამნაშავე და მათი რიცხვი უფრო და უფრო იზრდება. თავის მხრივ, მაღალშემოსავლიანი, პოტენციური დაზარალებულების რიცხვი მეტ-ნაკლებად უცვლელია, ისინი განთავსებულები არიან იდენტიფიცირებად და შედარებით განსხვავებულ (შემოსავლიან) ზონებში. შედეგად, პოტენციურ დაზარალებულებზე თავდასხმების ინტენსიურობა სავარაუდოდ კიდევ უფრო მოიმატებს. ინტერნეტმა მაღალშემოსავლიანი მსხვერპლი გახადა ისეთივე ხელმისაწვდომი დამნაშავეებისთვის, როგორც განვითარებად ქვეყნებში მცხოვრები მსხვერპლი. აღსანიშნავია, რომ თითოეულ ახალ დამნაშავეს შეუძლია მკვეთრად გაზარდოს შეტევების რიცხვი ავტომატიზაციის გამოყენებით. მრავალი მილიონი არასასურველი შეტყობინებების (ე.წ. „სპამის") დაგზავნა შესაძლებელია ავტომატურად, საკმაოდ მოკლე ვადაში. ჰაკერულმა თავდასხმებმაც ბოლო დროს მიიღეს ავტომატური ხასიათი, ყოველდღიურად ხორციელდება დაახლოებით 80 მილიონი ჰაკერული თავდასხმა, ძირითადად ავტომატიზაციის პროგრამების გამოყენებით, რომლებიც იძლევიან საშუალებას მიიტანონ იერიში ათასობით კომპიუტერულ სისტემაზე დროის მოკლე მონაკვეთში. ცოტა ხნის წინ, აღმოჩინეს ბოტნეტი, რომელშიც ჩართული იყო 12,7 მილიონი ინფიცირებული კომპიუტერი, მათ შორის მსოფლიოს უმსხვილეს კორპორაციების საკუთრებაში არსებული კომპიუტერები. მილიონობით თავდასხმის განხორციელების შესაძლებლობა მნიშვნელოვანია ორი მიზეზის გამო:

1. ეს ქმნის სიცოცხლისუნარიან და ეფექტურ კრიმინალურ სტრატეგიებს, რაც სხვაგვარად არ იქნებოდა სარგებლიანი ხარვეზების მაღალი მაჩვენებლების გამო. მაგალითად, თაღლითობისა და ფიშინგის არსებული სქემების შესახებ ინფორმირებულობის მიუხედავად, აღნიშნული სქემები შემოსავლიანია, ვინაიდან დამნაშავისთვის საკმარისია მილიონობით ცდაში ერთ ან ორ სამიზნემდე წარმატებით მიღწევა.
2. ეს აძლევს კიბერ-ქურდებს შესაძლებლობას არ მიიქციონ არასასურველი ყურადღება, ვინაიდან მცირე ოდენობის თანხის ქურდობა დიდი რაოდენობის მსხვერპლისგან ამცირებს გამოვლენის რისკებს.

ზოგიერთი ანალიტიკოსის მოსაზრებით 2008 წელს კიბერდანაშაულის შედეგად მიყენებული ზიანის ოდენობამ შეადგინა ერთი ტრილიონი აშშ დოლარი, თუმცა ბევრი არ ეთანხმებოდა ამ მოსაზრებას. საქმიანობის მასშტაბის და შესაძლო მსხვერპლთა რაოდენობის გათვალისწინებით (მსოფლიოში 2008 წლის მონაცემებით იყო 1,5 მილიარდზე მეტი ინტერნეტ მომხმარებელი), რთულია ზიანის ზუსტი განსაზღვრა და შეფასებების გაკეთება.[4]

კომპანია „LexisNexis"-ის 2019 წლის ანგარიშის მიხედვით მსოფლიო ლიდერი კიბერთავდასხმების განხორციელებაში არის ამერიკის შეერთებული შტატები, მას მოსდევენ კანადა, გაერთიანებული სამეფო, გერმანია და ირლანდია. ამავე ანგარიშის მიხედვით ბოლო ხუთი წლის მანძილზე კიბერდანაშაულმა განიცადა სახეცვლილება და კიდევ უფრო მეტად დაიხვეწა, შეიქმნა რთული თაღლითური სქემები. კიბერდანაშაული ჩამოყალიბდა დამოუკიდებელ დარგად. სპეციალისტები ვარაუდობენ, რომ აღნიშნული დანაშაული იქნება მომავალი ორი ათწლეულის ერთ-ერთი ყველაზე უფრო რთული გამოწვევა.[5]

შთამბეჭდავია კიბერდანაშაულის, როგორც კრიმინალური ბიზნესის შემოსავლები ციფრებში. 2012 წელს რუსეთის კიბერდანაშაულის გამოძიების კომპანიამ GROUP-IB გამოაქვეყნა კვლევა, რომლის თანახმადაც ამ ქვეყანაში კიბერდანაშაული წარმოადგენს 2.3 მილიარდ დოლარიან ბიზნესს.[6]

ანალიტიკოსები მიიჩნევენ, რომ 2015 წელს, ზოგადად, კიბერდანაშაულის შედეგად მიღებულმა შემოსავალმა შეადგინა 3 ტრილიონი აშშ დოლარი. ვარაუდობენ, რომ 2021 წლისთვის, კიბერდანაშაულის ინდუსტრიის შემოსავალი მიაღწევს წლიურად 6 ტრილიონ აშშ დოლარს.

---

4 United Nations Office on Drugs and Crime, The Globalization of Crime, A Transnational Organized Crime Threat Assessment, United Nations publication, Vienna, 2010, ISBN: 978-92-1-130295-0, pp 203-204 https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

5 The LexisNexis® Risk Solutions Cybercrime Report https://risk.lexisnexis.com/global/-/media/files/financial%20services/research/lnrs-cybercrime-report-research-january-june-2019.pdf

6 კოხრეიძე ნ. „რუსეთის კიბერ შესაძლებლობები" (კვლევა) http://ilawge.blogspot.com/2013/01/blog-post.html

როგორც დაიანგარიშეს, 2017 წელს Yahoo-ს სისტემაზე განხორციელებული კიბერშეტევა შეეხო დაახლოებით 3 მილიარდ ანგარიშს, Equifax-ზე განხორციელებულმა შეტევამ კი მოიცვა 145,5 მილიონი მომხმარებელი, რაც მიიჩნევა რეკორდულ მაჩვენებლად. იმავე წელს განხორციელდა კიდევ ორი მაშტაბური კიბერშეტევა WannaCry და NotPetya, აღნიშნული თავდასხმები არის არა მხოლოდ უფრო მაშტაბური, არამედ მინიშნება იმისა, რომ დროება იცვლება.[7]

IT-უსაფრთხოების დამოუკიდებელი ინსტიტუტის მონაცემებით, ყოველდღე, AV-TEST ინსტიტუტი არეგისტრირებს 350 000-ზე მეტ ახალ მავნე პროგრამას და პოტენციურად არასასურველ პროგრამას (PUA). რაც ფართოდ გამოიყენება კიბერშეტევის განხორციელებაში. 2011 წლის მონაცემებით ინსტიტუტმა, ერთ წელიწადში, გამოავლინა 65,26 მილიონი მავნე პროგრამა. შედარებისთვის 2020 წლის 15 ივლისის მონაცემებით, ანუ მხოლოდ ექვსნახევარ თვეში გამოვლინდა 1071,54 მილიონი ზიანის მომტანი პროგრამა. ეს მონაცემები ნათლად ადასტურებს, რომ კიბერდანაშაული წლების განმავლობაში მხოლოდ იხვეწება და აფართოებს მოქმედების არეალს.[8]

ყოველდღიურად, ინტერნეტ მომხმარებელთა მზარდი რიცხვი კიბერდანაშაულის შედეგად განიცდის ვიქტიმიზაციას. იმისათვის, რომ გაირკვეს, რამდენად სრულყოფილად გადიან რეაბილიტაციას კიბერდანაშაულის მსხვერპლები, მნიშვნელოვანია გავაცნობიეროთ აღნიშნული დანაშაულის ეფექტი და გავლენის ხარისხი. დღეის მდგომარეობით, კიბერდანაშაულის გავლენის საკითხზე საკმაოდ მწირე ინფორმაცია მოიპოვება. იმისათვის, რომ დაედგინათ თუ როგორ უნდა გავუმკლავდეთ კიბერდანაშაულის შედეგად ვიქტიმიზაციას, ჰოლანდიელმა მეცნიერებმა იურჯენ იანსენმა და რუთგერ ლუკფელდტმა ჩაატარეს საკმაოდ საინტერესო კვლევა, რომლის ფარგლებში გამოკითხეს 30 დაზარალებული პირი. კვლების შედეგად გამოვლინდა, რომ ფინანსურ ზარალთან ერთად, კიბერდანაშაული მსხვერპლზე ახდენს ფსიქოლოგიურ და ემოციურ ზეგავლენას. დაზარალებულებმა განაცხადეს, რომ დაექვემდებარნენ სხვადასხვა სახის მეორეხარისხოვან ზემოქმედებასაც, როგორიცაა, დროის დაკარგვა და არასათანადო მოპყრობა ინციდენტის გამოძიებისას. გარდა ამისა, დაზარალებულებში გამოვლინდა კოგნიტური და ქცევითი ცვლილებები.

საბოლოოდ კვლევის ავტორები მივიდნენ დასკვნამდე, რომ ისევე როგორც სხვა თაღლითობების შემთხვევაში, ინტერნეტ თაღლითობაც არ შეიძლება მივიჩნიოთ დანაშაულად მსხვერპლის გარეშე, იმ შემთხვევაშიც კი თუ ზიანის თანხა სრულად იქნება ანაზღაურებული. ამგვარი თაღლითური სქემების მოქმედება და გავლენა მსხვერპლზე არ უნდა დარჩეს არასათანადოდ შეფასებული. ინტერნეტ თაღლითობის შედეგად გამოწვეული ფინანსური დანაკარგებთან ერთად, დანაშაულის მსხვერპლს ეკარგება ნდობა (როგორც ონლაინ სერვისების, აგრეთვე ზოგადად ადამიანების) და ეუფლება დაუცველობის განცდა. ამასთან, რამდენად აღიქვამს ინდივიდი ამ ეფექტებს და გავლენას, ცალკეულ შემთხვევებში მნიშვნელოვნად განსხვავდება. ზოგისთვის ეს მხოლოდ დროებითი უხერხულობა იყო და მათ მოახერხეს მისი გადალახვა, ხოლო ზოგისთვის ეს იყო და რჩება დამთრგუნველ გამოცდილებად, რომელმაც ისინი შეცვალა. შედეგად ისინი გახდნენ უფრო ყურადღებიანები, ფხიზლები და გამსჭვალულები უნდობლობით. ეს ნიშნავს, რომ ინდივიდუალური განსხვავებები უნდა იქნას გათვალისწინებული, როდესაც დაზარალებულებს ეხმარებიან გაუმკლავდნენ მათ ვიქტიმიზაციას. აქედან გამომდინარე, იმისათვის, რომ დახმარება იყოს ეფექტური, უნდა გათვალისწინებულ იქნას ურთიერთქმედება დაზარალებულის პიროვნულ მახასიათებლებსა და გარემოს შორის.[9]

კიბერდანაშაულის მჭიდროდ არის დაკავშირებული ინტერნეტთან, იმ მარტივი მიზეზით, რომ ინტერნეტის გარეშე ის ვერ იარსებებდა. სწორედ ინტერნეტი ქმნის იმ ციფრულ გარემოს, რომელიც სასიცოცხლოდ მნიშვნელოვანია ამ დანაშაულისათვის. თავის მხრივ ინტერნეტი არ უნდა მივიჩნიოთ ტექნოლოგიის ერთ-ერთ ჩვეულებრივ გამოვლინებად, რომელიც არსებობს იმ ადამიანებისგან დამოუკიდებლად ვინც მას იყენებს. უფრო მეტიც, ის უნდა განიხილებოდეს, როგორც სოციალური აქტივობების ერთობლიობა, ვინაიდან ადამიანები მას იყენებენ კონკრეტული გზით და კონკრეტული მიზნებისთვის.

7 Cybersecurity Ventures, 2017 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

8 The independent IT-security institute, AV-TEST GmbH, Magdenburg, Germany https://www.av-test.org/en/statistics/malware/

9 Jansen J., Leukfeldt R., Coping with cybercrime victimization: An exploratory study into impact and change, Journal of Qualitative Criminal Justice and Criminology, volume 6, Number 2, Special Issue, Dallas, 2018, pp 223-224; https://www.jqcjc.org/documents/v6i2.pdf#page=78

ინტერნეტის საზოგადოებრივი მიზნებისთვის გამოყენებით სამოქმედო არეალი იქმნება სხვა და სხვა სახის დანაშაულებრივი და უკანონო საქმიანობისთვის. მაგალითისთვის, ადამიანებს რომ არ გამოეყენებინათ ინტერნეტი ვაჭრობისთვის, საკრედიტო ბარათებთან დაკავშირებული დანაშაულების ჩასადენად საჭირო პერსონალური ინფორმაცია არ იქნებოდა ხელმისაწვდომი დამნაშავეთათვის. ანალოგიურად, როდესაც ჩვენ ვიყენებთ ინტერნეტს და ელექტრონულ ფოსტას მეგობრებთან თუ თანამშრომლებთან კომუნიკაციისთვის, სპეციალური პროგრამების გამოყენებით შესაძლებელი ხდება საფოსტო სისტემებში შეღწევა და მონაცემების მოპარვა. ინტერნეტის გამოყენების ერთ-ერთი ყველაზე მნიშვნელოვან სფეროს წარმოადგენს საქმიანი ურთიერთობები და ბიზნესი. ინტერნეტი ფართოდ გამოიყენება ჩვეულებრივი საქმიანი ურთიერთობებისთვის, დაწყებული ბაზრის კვლევით და დასრულებული წარმოებით, დისტრიბუციით, მარკეტინგით და გაყიდვებით. აღნიშნული თავის მხრივ ქმნის შესაძლებლობებს კრიმინალური აქტივობებისთვის, მაგალითად სავაჭრო საიდუმლოების და სტრატეგიული ინფორმაციის ქურდობა, ონლაინ სავაჭრო სისტემების შეფერხება, საბარათე მონაცემების თაღლითურად გამოყენება საქონლის და მომსახურების შესაძენად. ონლაინ ბანკინგის და მსგავსი მომსახურებების განვითარებამ ასპარეზი გაუხსნა ფინანსური დანაშაულების ახალ სახეებს, რა დროსაც გამოიყენება პიროვნების დადგენის სისტემების მოტყუების ახალი მეთოდები. გარდა ამისა ინტერნეტი უფრო და უფრო აქტიურად გამოიყენება პოლიტიკური მიზნებისთვის, მთავრობები ინტერნეტს იყენებენ მოქალაქეების ინფორმირების და კონსულტაციის მიზნით, პოლიტიკური პარტიები იყენებენ მას მხარდაჭერების მოზიდვისთვის, ცალკეული საინიციატივო ჯგუფები ინტერნეტს იყენებენ კამპანიების წარმართვის და თანხების შესაგროვებლად და სხვა. შესაბამისად, ჩნდება ახალი ტიპის კიბერდანაშაულები, რომლებიც ატარებენ პოლიტიკურ ხასიათს, რაც გამოიხატება ოფიციალური ვებ-გვერდების საბოტაჟში, ექსტრემისტების მიერ სიძულვილით მოტივირებული კამპანიების წარმართვაში და ტერორისტული დაჯგუფებების მიერ ახალი წევრების რეკრუტირებაში და დაფინანსების მოზიდვაში. ინტერნეტის გამოყენების კიდევ ერთი საშუალებაა დასვენება და კულტურული ღონისძიებები, როგორიცაა მუსიკა, კინო და ვიდეო თამაშები. აღნიშნულ საქონელზე და მომსახურებაზე მოთხოვნის ზრდასთან ერთად, ამ მიმართულებით გაიზარდა კრიმინალური აქტივობაც, რაც გამოიხატება პირატური პროგრამული უზრუნველყოფით, აუდიო და ვიდეო ჩანაწერებით ვაჭრობაში. საზოგადოების მხრიდან ინტერნეტის გამოყენების კიდევ ერთი თვალსაჩინო მაგალითია სოციალური ქსელები და მედია პლატფორმები (Facebook, Twitter, Instagram), რაც თავის მხრივ წარმოშობს ახალ შესაძლებლობებს კიბერდანაშაულისთვის. ზემოხსენებული გახლავთ კიბერდანაშუალის ჩადენის არეალის მხოლოდ ნაწილი, ვინაიდან ინტერნეტმა მოიცვა ადამიანის ცხოვრების თითქმის ყველა სფერო და გახდა მისი განუყოფელი ნაწილი.[10]

დანაშაული სოციალურ ფენომენად მიიჩნევა, კიბერდანაშაული თავის მხრივ სოციალურ-ეკო-პოლიტიკური ხასიათის მატარებელია, ვინაიდან მან მოიცვა საზოგადოებრივი ურთიერთობების საკმაოდ ფართო სპექტრი. თითქმის არ დარჩა სფერო და საზოგადოების ფენა, რომელიც არ ზარალდება აღნიშნული დანაშაულის შედეგად, იგი გავლენას ახდენს კერძო და საჯარო სექტორებზე, ბიზნესზე, მომხმარებლებზე, მოზარდებზე (კიბერ ბულინგი, ბავშთა პორნოგრაფია და სხვა) და ზოგადად ადამიანის ფსიქოლოგიურ მდგომარეობაზე.[11]

2018 წელს, დიდი ბრიტანეთის შინაგან საქმეთა სამინისტრომ ჩაატარა კვლევა კიბერდანაშაულის შედეგად წარმოშობილი ხარჯების დაანგარიშების მიზნით. დაანგარიშებულ იქნა ამ დანაშაულისგან მომდინარე მოსალოდნელი ხარჯები, შედეგად მიღებული ხარჯები და საპასუხო ხარჯები. საბოლოოდ გათვალისწინებულ იქნა არა მხოლოდ უშუალოდ დანაშაულის შედეგად მიყენებული ზიანის ოდენობა, არამედ დანაშაულთან ეფექტური ბრძოლისთვის გასატარებელი ღონისძიებებიც. ხარჯებს შორის მოექცა დაცვის ახალი ტექნოლოგიების განვითარებისთვის საჭირო ხარჯები, კვალიფიკაციის ასამაღლებელი ტრენინგები, ციფრული უსაფრთხოების გაზრდის მიზნით გასატარებელი ღონისძიებები და ახალი ქცევის პროტოკოლები, ახალი ტიპის კანონმდებლობის შემუშავებისა და იმპლემენტაციის ხარჯები, თავდასხმების შედეგად დაზიანებული ტექნიკის და ინვენტარის აღდგენის ხარჯები, აგრეთვე სამართალდამცა-

10 Yar M., Steinmetz K.F., Cybercrime and Society, Third Edition, SAGE Publishing Ltd, London, 2019 p. 7-9

11 Sumanjit D., Tapaswini N., Impact of Cyber Crime: Issues and Challenges, International Journal of Engineering Sciences & Emerging Technologies, Volume 6, Issue 2, pp: 147-151 http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf

ვი, სასამართლო და პენიტენციური ორგანოების მხრიდან გაწეული დანახარჯები. კვლევის ავტორების შეფასებით კიბერდანაშაულის შედეგად წარმოშობილი ხარჯები შეადგენს დაახლოებით 27 მილიარდ ფუნტს ყოველწლიურად, მათ შორის სახელმწიფო ხარჯები 2,2 მილიარდი ფუნტი, მოქალაქეებისთვის მიყენებული ზიანი – 9,1 მილიარდი ფუნტი და ბიზნეს სექტორის ზიანი – 16 მილიარდი ფუნტი.[12]

2000 წლის მაისში, ამერიკის შეერთებული შტატების ფედერალურ საგამოძიებო ბიუროში შეიქმნა სპეციალური ცენტრი – IC3, რომელშიც აკუმულირდებოდა ინტერნეტ დანაშაულის თაობაზე შესული საჩივრები. ცენტრის მიზანია მსოფლიო მასშტაბით განხორციელებული, შესაძლო ინტერნეტ დანაშაულის თაობაზე შეტყობინებების მიღება და დამუშავება, შემდგომში ეფექტური ბრძოლის მეთოდების შემუშავებისა და გამოძიების ეფექტურობის ამაღლების მიზნით. მიღებული ინფორმაციის დამუშავების და გაანალიზების შემდეგ ცენტრი ადგენს ყოველწლიურ მოხსენებას, რომელიც ხელმისაწვდომია ფართო საზოგადოებისათვის. აღნიშნული ემსახურება საზოგადოებრივი ცნობიერების ამაღლებასა და ინფორმირებას.

2019 წლის ანგარიშის მიხედვით, შექმნის დღიდან, ანგარიშის გამოქვეყნების მომენტამდე, მხოლოდ ზემოაღნიშნულ სამსახურში შევიდა 4,883,231 შეტყობინება. მხოლოდ წინა 5 წლის მონაცემებით ზიანის სავარაუდო ოდენობა შეადგენდა 10,2 მილიარდ აშშ დოლარს.

ამავე ანგარიშში მოყვანილია 20 ქვეყანა, რომელიც 2019 წლის მონაცემებით ლიდერობს კიბერდანაშაულის მსხვერპლთა საერთო რაოდენობით (IC3-ში შესული შეტყობინებების მიხედვით). პირველ ადგილზე გვევლინება გაერთიანებული სამეფო (93,796 შემთხვევა). ანგარიშის მიხედვით 2019 წლის მონაცემებით საქართველო იკავებს მე-14 ადგილს. საქართველოში დაფიქსირდა 454 შემთხვევა. ამ მონაცემების მიხედვით საქართველო უსწრებს შვეიცარიას (438 შემთხვევა), იტალიას (428 შემთხვევა), ჩინეთს (403 შემთხვევა), მალაიზიას (362 შემთხვევა), ესპანეთსა (358 შემთხვევა) და რუსეთის ფედერაციას (349 შემთხვევა).[13]

2019 წელს მოსკოვში გაიმართა კიბერუსაფრთხოების საერთაშორისო კონგრესის მორიგი შეხვედრა. კიბერუსაფრთხოების საერთაშორისო კონგრესი, ერთ – ერთი მთავარი სპეციალიზებული მოვლენა და უნიკალური პლატფორმაა, რომელიც აერთიანებს მთავრობის წარმომადგენლებს, მსოფლიო ბიზნესის ლიდერებსა და ინდუსტრიის აღიარებულ ექსპერტებს. გონგრესზე ღია დიალოგის ფარგლებში მსჯელობენ კიბერუსაფრთხოების ყველაზე აქტუალურ და გლობალურ საკითხებზე.

კონგრესის შედეგების მიხედვით, 2019 წლის მდგომაროებით ყველაზე აქტუალური მიმართულება ახალი ტექნოლოგიების სფეროში იყო კიბერუსაფრთხოება, როგორც ციფრული ეპოქის ერთ-ერთი მთავარი საკითხი და მთავარი გამოწვევა. კონგრესზე დადგინდა, რომ კიბერ საფრთხეებისგან დაცვისთვის, პრევენცია უფრო ეფექტური იყო, ვიდრე თავდასხმის შემდგომი შედეგების აღმოფხვრა, თუმცა აღინიშნა, რომ ამ კატეგორიის დანაშაულის პრევენცია დიდ ინვესტიციებს მოითხოვდა. გამოვლინდა, რომ ბოლო დროს ტექნოლოგიურ და ფინანსური სექტორში საქმიანობის განმახორციელებელი კომპანიები და სახელმწიფო უწყებები ყველაზე აქტიურად ინვესტიციას დებენ სწორედ კიბერ უსაფრთხოებაში. უფრო მეტიც, ბანკები და სამთავრობო ორგანიზაციები, აცნობიერებენ რა საფრთხის მასშტაბებს, არ ზღუდავენ ხარჯებს ამ მიმართულებით. ბოლო 13 წლის მონაცემებით კიბერუსაფრთხოების სფეროში ინვესტირების მაჩვენებელი გაიზარდა 35-ჯერ და მხოლოდ 2017 წელს შეადგინა 120 მილიარდი აშშ დოლარი. ამავე კონგრესის მონაცემებით მსოფლიოში არის 4 მილიარდი ინტერნეტმომხმარებელი, ხოლო მობილური ტელეფონების მომხმარებელთა რიცხვი შეადგენს 5 მილიარდს.[14]

როგორც ვხედავთ კიბერდანაშაულის შედეგად მიყენებული ზიანი მზარდია და წლიდან წლამდე კოლოსალურ მატერიალურ ზიანს აყენებს არა მხოლოდ კერძო სამეწარმეო სუბიექტებისა და მოქალაქეების კანონიერ ინტერესებს, არამედ სახელწიფო ინსტიტუტების გამართულ ფუნქციონირებასა და საბანკო თუ საფონდო ბირჟების საქმიანობას. აღნიშნული კვლევები და დასკვნები ცხადად წარმოაჩენს, რომ კიბერდანაშაულზე ქმედითი რეაგირება უნდა ატარებდეს კომპლექსურ ხასიათს, უნდა

12 Understanding the costs of cyber crime, A report of key findings from the Costs of Cyber Crime Working Group, Research Report 96, Home Office Science Advisory Council, January 2018, pp 25-26
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf

13 Federal Bureau of Investigation Internet Crime Complaint Center, 2019 crime complaint report, pp. 5, 17
https://pdf.ic3.gov/2019_IC3Report.pdf

14 2019 International Cybersecurity Congress report, p. 87
https://icc.moscow/upload/doc/ICC_reports_EN.pdf

ეფუძნებოდეს ერთიან, ჯეროვნად ჩამოყალიბებულ საერთაშორისო პოლიტიკას, რისი მიღწევაც მხოლოდ სახელმწიფოთაშორისი მჭიდრო თანამშრომლობისა და მყისიერი (ბიუროკრატიული ფორმალიზმის გვერდით ავლით) ურთიერთ სამართლებრივი დახმარების გაწევის გზით არის შესაძლებელი. ცალკეულ, თუნდაც ძლიერი ეკონომიკისა და მაღალტექნოლოგიური განვითარების ქვეყნებში, რომელიმე სფეროს, ან დანაშაულთან ბრძოლის კონკრეტული მიმართულებების დახვეწა/განვითარება ვერ უზრუნველყოფს დანაშაულის პრევენციასა და მასზე ეფექტურ რეაგირებას, ვინაიდან კიბერდანაშაული გლობალური და ტრანსნაციონალური ხასიათის დანაშაულია და მისგან მომდინარე საფრთხეები შემაშფოთებლად მზარდია.

ბიბლიოგრაფია:

1. ცაცანაშვილი მ., სიხარულიძე ტ., კიბერტერორიზმის პრობლემები სამათალში, ელ. ჟურნალი „კიბერ უსაფრთხოება", 2007 წ. http://informsoc.org/ka/journal/cybersecurity/69-2009-08-19-15-33-04
2. კოხრეიძე ნ. „კიბერდანაშაული". http://ilawge.blogspot.com/2012/05/blog-post_191.html
3. კოხრეიძე ნ. „რუსეთის კიბერ შესაძლებლობები" (კვლევა)http://ilawge.blogspot.com/2013/01/blog-post.html
4. ლანჩავა გ. „კომპიუტერული დანაშაული", ჟურ. „მართლმსაჯულება", N2, 2008 წ.
5. Yar M., Steinmetz K.F., Cybercrime and Society, Third Edition, SAGE Publishing Ltd, London, 2019.
6. United Nations Office on Drugs and Crime, The Globalization of Crime, A Transnational Organized Crime Threat Assessment, United Nations publication, Vienna, 2010, ISBN: 978-92-1-130295-0 https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf
7. The LexisNexis® Risk Solutions Cybercrime Report https://risk.lexisnexis.com/global/-/media/files/financial%20services/research/lnrs-cybercrime-report-research-january-june-2019.pdf
8. Cybersecurity Ventures, 2017 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
9. The independent IT-security institute, AV-TEST GmbH, Magdenburg, Germany https://www.av-test.org/en/statistics/malware/
10. Jansen J., Leukfeldt R., Coping with cybercrime victimization: An exploratory study into impact and change, Journal of Qualitative Criminal Justice and Criminology, volume 6, Number 2, Special Issue, Dallas, 2018 https://www.jqcjc.org/documents/v6i2.pdf#page=78
11. Sumanjit D., Tapaswini N., Impact of Cyber Crime: Issues and Challenges, International Journal of Engineering Sciences & Emerging Technologies, Volume 6, Issue 2. http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
12. Understanding the costs of cyber crime, A report of key findings from the Costs of Cyber Crime Working Group, Research Report 96, Home Office Science Advisory Council, January 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf
13. Federal Bureau of Investigation Internet Crime Complaint Center, 2019 crime complaint report https://pdf.ic3.gov/2019_IC3Report.pdf
14. 2019 International Cybersecurity Congress report https://icc.moscow/upload/doc/ICC_reports_EN.pdf